UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,038	01/30/2004	Daniel M. Bodorin	MSFT122168	7942

26389 7590 05/01/2007
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER
NGUYEN, KHOI

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/769,038	**Applicant(s)** BODORIN ET AL.	
	Examiner Khoi Nguyen	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-4 are pending and presenting for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless – (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-4 are rejected under 35 USC 102(b) as anticipated by White et al. ("Anatomy of a Commercial-Grade Immune System", http://citeseer.ist.psu.edu/white99anatomy.html, 1999), hereafter "White".

> *Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.*

4. With regard to claims 1 and 2, White discloses a malware detection system and means for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the system comprising:

at least one dynamic behavior evaluation module (Fig. 6, page 20, Analysis Center reads on dynamic behavior evaluation module), wherein each dynamic behavior evaluation module provides a virtual environment in which a code module of a particular type may be executed (Section "Creation of the replication environment", Page 20: paragraph 1: lines 1-5), and wherein each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature (Fig. 6, page 20: item "archive" and Section "Analysis", page 21: paragraph 1: lines 5-6, extract good signature and stores in the archive for developing virus definition reads on each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature);

a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type (Fig. 3: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type);

a malware behavior signature store storing at least one known malware behavior signature (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on malware behavior signature store storing at least one known malware behavior signature); and a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware).

5. With regard to claim 3, White discloses a method for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module (Fig. 3: page 20: item "workflow supervisor", page 19: paragraph 1 and 2, and Section "Macro Viruses", page 25: paragraph 1: lines 5-7, supervisor selects sample and dispatch to the particular system as described in Section "Marco viruses" reads on selecting a dynamic behavior evaluation module according to the executable type of the code module);

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed (Section "Creation of the replication environment", Page 20: paragraph 1 and 2);

recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module);

comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15:

paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors); and

according to the results of the previous comparison, determining whether the code module is malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 3: lines 1-6, gateway scans the sample to see if it can handle the sample by itself reads on according to the results of the previous comparison, determining whether the code module is malware).

6. With regard to claim 4, White discloses a computer-readable medium bearing computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors (Fig. 5: page 18) , the method comprising

selecting a dynamic behavior evaluation module according to the executable type of the code module (Fig. 3: page 20: item "workflow supervisor", page 19: paragraph 1 and 2, and Section "Macro Viruses", page 25: paragraph 1: lines 5-7, supervisor selects sample and dispatch to the particular system as described in Section "Marco viruses" reads on selecting a dynamic behavior evaluation module according to the executable type of the code module);

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed (Section "Creation of the replication environment", Page 20: paragraph 1 and 2);

recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads on recording some behaviors exhibited by the code module executing in the dynamic behavior evaluation module);

comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on comparing the recorded behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware behaviors); and according to the results of the previous comparison, determining whether the code module is malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 3: lines 1-6, gateway scans the sample to see if it can handle the sample by itself reads on according to the results of the previous comparison, determining whether the code module is malware).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US Pat. No. 6357008 to Nachenberg (Discloses a virus detection through 3 stages by emulate a number of instructions to allow an encrypted virus to decrypt itself).

b. US Pat. No. 5485575 to Chess et al. (Discloses information pertaining to the verification and transformation of a computer virus).

c. US PGPub No. 20040015712 to Szor. (Discloses a Virtual Machine to detect a computer virus in a host file).

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251.

The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

9. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 4/24/07

Benjamin E. Lanier
Examiner AU2132